ABSTRACT:

In a method for providing copy-protection services on a storage medium (for instance a solid state memory module), the data are arranged in sectors to which a field (S4T) is associated, where said field contains a random value R_i which is changed randomly when writing data to said sector. By encrypting the data stored on the medium using a key which depends critically on said random numbers, bit-by-bit copies (apart from said random numbers, which can not be deterministically changed by an application) to a second storage medium or recopies from some intermediate storage medium, can not be decrypted because the values of said random numbers will have changed, thus preventing unauthorized duplication and replay attacks.